S.I. Files

C.P. & T.Div.

WAR DEPARTMENT
SIG
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

August 21, 1931

MEMORANDUM FOR: Research and Development Division.

1. There is enclosed a draft of the specifications and claims applicable to the cipher machine now being developed at the laboratories. There is also enclosed a drawing which accompanies the specifications and claims.

2. These were drawn up by Mr. Friedman and represent his ideas with regard to a proper description suitable for forming a basis for application for a patent covering the machine. At the same time these should be regarded as tentative and this Division will appreciate any changes, comments or criticisms deemed advisable by the laboratories. For these reasons it is suggested that these enclosures be forwarded to the laboratories without delay.

D. M. Crawford,
Major, Signal Corps.

2 Enclosures:
Specifications and claims,
1 Drawing.

D R A F T

The object of this invention is to provide a cryptograph for enciphering and deciphering messages automatically, rapidly, and securely.

A further object of this invention is the provision of a cryptograph controlled by a modified plural-unit-code tape transmitter through which is passed a key tape which serves as the keying element in the encipherment or decipherment of messages.

A further object of this invention is the provision of a cryptograph, which, although employing for its keying element a plural-unit-code of the Baudot type (a code of 32 permutations), nevertheless produces cryptograms the characters of which are restricted to the 26 letters of the alphabet. In this respect the cryptograph excludes the usual six extra Baudot characters, the transmission of which occasions much difficulty in ordinary telegraphy by the Morse alphabet. The way in which these six extra characters are eliminated constitutes one of the unique and important features of our invention.

A further object of this invention is to provide a cryptograph adapted to function either independently as a self-contained cryptographic unit, or in conjunction with an independent typewriter having a standard typewriter keyboard. In the first case, the cryptograph makes no permanent record of the message, but merely produces evanescent signals such as light signals; in the second case, the cryptograph brings about the making of a written

record of the message.

A further object of this invention is the provision of a cryptograph functioning at the transmitting end of a communication system as a means for indirectly controlling a telegraph transmitter keyboard, so that the intelligence to be transmitted is automatically enciphered before transmission; and similarly, at the receiving end, a corresponding cryptograph functions as a means for indirectly controlling an ordinary typewriter so that the intelligence received in cryptographic form is deciphered before being typed by the typewriter.

By way of an introductory statement to our invention, it may be said that in practically all the portable mechanical, electrical, or mechanico-electrical cryptographing devices or systems heretofore devised, the cryptographing and decryptographing of messages is entirely controlled by elements all embodied within the mechanism itself; that is, the basic, or invariable elements concerned in the cryptographic treatment, as well as the keying, or variable elements for controlling the cryptographic treatment are integral parts of the device or apparatus. In contradistinction to this situation, in our invention, only the basic, or invariable elements concerned in the cryptographic treatment are integral parts of the mechanism, the keying, or variable elements being wholly independent of the mechanism itself, and consist of an extraneous factor which when properly associated with the mechanism con-

trols the basic or invariable elements of the mechanism in cryptographing and decryptographing messages.

In the drawings accompanying and forming a part of this application, Figure 1 is a schematic representation of the cryptograph; Figure 2 is a side elevation view, and Figure 3 is a plan view of the cipher wheel which is one of the important elements in the cryptographing mechanism.

It is believed that an explanation of the schematic representation of our invention will form the best basis for its understanding, and therefore reference will be made to Figure 1. In this figure, 1 represents the keyboard of the cryptograph, the arrangement of the 26 keys thereof being that of the standard typewriter keyboard except that only 26 keys corresponding to the 26 letters of the alphabet are included. Each key of the keyboard operates an electrical contact, as shown schematically for the "Q" and "W" keys. In addition, our keyboard is provided with a universal bar which is actuated with each depression of any key. Keyboards of this type are well known in the art and require no further description.

The cipher wheel is shown at 2 in Figure 1. It may be made of bakelite or similar material, and serves as a commutator for carrying 52 brush-type contacts arranged in two rings or sets of 26 each, one set being placed on the obverse face, 3, of the wheel 2, the other set being similarly placed on the reverse face, 5, of the wheel. The 26 contacts on each face are arranged equidistantly from one another in a circle around the periphery of the face,

the contacts on the obverse face being connected to those on the reverse face by means of flexible, insulated conductors which pass through the interior of the wheel, as shown schematically in Figure 1 for two pairs of contacts. The cipher wheel is fixed upon the shaft 7, which serves as an axis on which the wheel may revolve. The contacts of the obverse face, 3, of the cipher wheel press against ball-bearing type contacts arranged on the fixed plate 4; the contacts of the reverse face, 5, of the cipher wheel press against ball-bearing type contacts arranged on the fixed plate 6. The fixed plates 4 and 6 each contain 26 contacts arranged equidistantly in a circle. The cipher wheel revolves between these fixed plates 4 and 6 so that each contact on the obverse face, 3, of the cipher wheel presents itself in turn to each contact on plate 4, and each contact on the reverse face, 5, of the cipher wheel presents itself in turn to each contact on plate 6, as the cipher wheel revolves. The contacts of plate 6 are respectively connected by conductors to the contacts of the keyboard 1; the contacts of plate 4 are respectively connected by conductors to a bank of 26 electrical elements which may be small lamps, relays, or solenoids, only two of which are shown at 10. For the sake of simplicity of explanation, it will be assumed that the electrical elements in this bank are lamps. As shown in Figure 1, when the key "Q" is depressed, assuming the cipher wheel to be in the position indicated in the figure, a circuit is established as follows: From positive pole of battery 11 through conductor 12, closed contact at the "Q" key, conductor 13, contact 14 on fixed plate 6, contact 15 on cipher wheel

2, conductor 16, contact 17 of cipher wheel 2, contact 18 of plate 4, conductor 19, through lamp 20, conductor 21 to negative of battery 11. Lamp 20 has a translucent glass window before it, on which a letter is painted, say the letter "W". Hence, depression of the key "Q" on the keyboard gives the cipher resultant "W", under the conditions specified.

Suppose that the key "W" of the keyboard is depressed, instead of "Q". By following the path set up for the electrical current, it will be seen that the "Q" lamp will be lighted. Thus, reciprocity is established between the keys on the keyboard and the lamps so that if, for example, Q = W, in enciphering, W = Q in deciphering. The same reciprocal relationship can be established throughout the alphabet by connecting the flexible conductors in the interior of the cipher wheel in an appropriate manner to paired contacts on the obverse and reverse faces of the cipher wheel.

If the cipher wheel were stationary, the relationship between the key depressed and the lamp illuminated, that is, in the equivalence between plain-text and cipher letters, would be fixed for each wiring of the interior of the cipher wheel. But the cipher wheel is rotatable and hence this relationship is subject to variation. As thus far described our cipher wheel is by no means novel in the art, similar wheels being well known in other cryptographs. Our cipher wheel is, however, novel in respect to certain features connected with the way in which the relationship between plain-text and cipher letters is

varied and controlled, and these features will now be presented.

The rim or tire of our cipher wheel, 2, is provided with 130 pins arranged in five superimposed bands, each band consisting of 26 equidistantly-spaced pins. These pins can be elevated into operative positions or left remaining in inoperative positions in groups of fives transversely to the tire, in accordance with the permutations of the 5-unit or Baudot code. To explain what is meant, we may say that according to the Baudot code, the permutation of elements for the letter A, for example, is represented thus:

1 2 3 4 5
/ / _ _ _. For our purposes we will let the / sign indicate that a pin is to be elevated into its operative position, the - sign, that it is to be left in its inoperative position. In Figure 2 there is shown a side elevation view of a section of the tire of the cipher wheel, with the pins now being described. The pins indicated by dotted lines in the figure represent pins which have been left depressed in their inoperative positions; the pins indicated by whole lines represent pins which have been elevated into their operative positions. The permutations represented in Figure 2 correspond to the Baudot signals for the letters Y, Z and A. The order of the letters in Figure 2, is, of course, only illustrative, since all the pins can be arranged in operative or inoperative positions to correspond with any sequence of signals of the Baudot code, and hence this sequence may be varied at will.

The function of the pins on the rim of the cipher wheel is to control the

cipher-wheel transmitter shown at 22 in Figure 1, which consists essentially of a set of 5 contact-levers moveable between paired left and right contacts. Normally, these contact-levers are held against the left contact, by the action of respective retractile springs, but when a pin on the rim of the cipher wheel is in its operative position and can therefore present itself to the contact-lever with which it is associated, it presses against the contact-lever and causes it to make contact at the right. Pins in their inoperative position do not, of course, act upon these contact-levers, allowing the latter to remain against their respective left-hand contacts. The function of the paired contacts controlled by the respective contact-levers of the cipher-wheel transmitter will be explained presently.

On the rim of the cipher wheel, and near the edge of the reverse face, 5, there is a ratchet wheel, shown in Figure 3. This ratchet wheel contains 26 equidistantly-spaced teeth, only five of which are shown in Figure 3, one tooth being labeled 23. It is likewise labeled 23 in Figure 1. Associated with the ratchet wheel is the pawl shown at 24, Figures 1 and 3. The ratchet wheel and pawl, together with solenoid 25 and its armature 41, Figures 1 and 3, control the movement of the cipher wheel in its rotation about the axis, 7, under the drive of coiled spring 8, which is wound by a motor not shown in the drawing. The movement of the cipher wheel is step-by-step, at intervals which will be explained subsequently in discussing the way in which the whole system functions.

The key-tape transmitter, 26, Figure 1, is a slightly modified Baudot code transmitter such as is employed with printing telegraph equipment of the Western Electric or Morkrum type. Its general features need not be explained, similar transmitters being well known in the art. It is sufficient to say here that a tape containing perforations permuted in accordance with the Baudot Code is passed through this transmitter, setting up a series of 5 contacts inside the transmitter in accordance with the Baudot Code. The transmitter is, of course, also provided with a tape-stepping magnet, 27, the function of which is to step the tape forward at proper intervals. The principal difference between the transmitter as used in standard printing telegraph equipment and as used in our invention consists in the way in which the left and right paired contacts of the normal Baudot tape transmitter are interconnected. In the normally-wired transmitter the five contact-levers and their ten associated, paired contacts are members of a set of five separate or independent circuits; in the transmitter as modified for our purposes the five contact-levers and their ten associated paired contacts are members of a single circuit, as is explained in the next paragraph.

The key-tape transmitter, 26, is associated and functions jointly with the cipher-wheel transmitter, 22, to control the angular displacements of the cipher wheel in the following manner. Note relay 28, which is energized by current from battery 29, through a path which begins at conductor 30 and includes only

ten of the twenty contacts and all the contact-levers of cipher-wheel transmitter, 22, and key-tape transmitter, 26, and emerges along conductor 31. Note also the illustrative set-up of contacts and contact-levers at 22 and 26 in Figure 1, in which a specific case is presented. It is assumed there that the arrangement of operative pins on the cipher wheel which are at that moment presenting themselves to the contact-levers of the cipher-wheel transmitter, 22, corresponds to the Baudot permutation for letter "Z". At the same moment the character on the key tape and the permutation of contacts set-up within the key-tape transmitter, 26, also corresponds to the letter "Z". Note that in view of the manner in which the twenty contacts and the ten contact-levers of 22 and 26 are interconnected, the circuit from battery 29 through relay 28 is completed only when the whole set of electrical connections established at the key-tape transmitter, 26, coincides with the whole set of connections established at the cipher-wheel transmitter, 22. Hence, if "Z" is set up in key-tape transmitter, 26, relay 28 will operate only when "Z" is set up in the cipher-wheel transmitter, 22. Similarly if any other letter, say "X", is set up in the key-tape transmitter, 26, relay 28 will operate only when "X" is set up in the cipher-wheel transmitter, 22. The complete path of the current when such coincidence of connections in transmitters 22 and 26 is established is as follows:

From positive of battery 29 along conductor 30, through all the contact-

levers and the ten associated closed contacts of transmitters 26 and 23, conductor 31 to back contact 32, of armature 33, winding of relay 28, conductor 34, to negative of battery 29. It is obvious that since the armature 33 and back contact 32 of relay 28 form parts of the circuit for energizing relay 28, as soon as the relay has received an impulse and armature 33 is attracted, the circuit for energizing relay 28 is broken at contact 32. Since armature 33 is under tension of a retractile spring, if not prevented from being pulled back into its normal position on release of relay 28, armature 33 would reestablish contact at 32 and would set up a chattering. But the mechanical arrangements are such that when armature 33 is first drawn up by relay 28 it passes by and is immediately engaged by lever 35 and held from returning to its retracted position where it can reestablish contact at 32, until lever 35 is displaced by mechanical action to be described later. Armature 33 of relay 28 also controls the solenoid 25, already referred to, which, in turn, controls the rotation of the cipher wheel, 2, in the following manner:

The motor-operated coiled spring, 8, tends to rotate the cipher wheel in the direction indicated by the arrow, say to the right. This rotation is step-by-step, controlled by the solenoid 25, and the ratchet referred to above. Assume the contact-levers in transmitters 22 and 26 set up to different permutations so that relay 28 is not energized and hence contact 36 is closed. A current starts from positive of battery 37 through conductor 38, closed contact

36, conductor 39, back contact 40, armature 41, conductor 42, winding of solenoid, 25, conductor 43, to negative of battery 37. A momentary impulse passes through 25 and causes armature 41 to be attracted, breaking the circuit at back contact 40, whereupon armature 41, under action of its spring, returns and again closes the circuit at 40. However, the mechanical arrangement is such that the momentary attraction of armature 41 releases the pawl, 24, associated with the ratchet on the cipher wheel and thus allows the cipher wheel, driven by coiled spring, 8, to advance one step. Thus, the cipher wheel continues to move, one step at a time, so long as back contact 36 of relay 28 remains closed. When, however, the permutation of contacts set up in the cipher-wheel transmitter becomes the same as that set up in the key-tape transmitter, thus causing the completion of the circuit through relay 28 as already described, and thus, when contact 36 is opened, under the action of relay 28, and is held open by lever 35 as described above, solenoid 25 cannot operate to withdraw armature 41; hence the pawl 24 cannot be released, whereupon the cipher wheel cannot advance any further. As stated before, the first impulse through relay 28 causes armature 33 to be attracted, to pass by lever 35, which then engages the armature. Thus contact 36 remains open as long as lever 35 engages and holds it. It is only within this period, when the cipher wheel is stationary, that the keyboard, 1, can be manipulated, the mechanical arrangement being such that the keys of the keyboard are locked except when the cipher wheel is stationary.

Suppose now a key is depressed. The cipher resultant will be determined by the position of the cipher wheel at this time, because the circuit established through the cipher wheel depends upon the exact relative position of this wheel with respect to fixed plates 4 and 6. When a key is depressed, the cipher resultant is shown by the illuminated lamp; the latter continues to be illuminated so long as the key is held down.

We return now to relay 28 and its other armature 46. The latter controls the operation of the tape-stepping magnet 27 of the key-tape transmitter 26, in the following manner:

The tape-stepping magnet 27 is actuated by battery 44, but the circuit is normally open at contact 45. When armature 46 is attracted and relay 28 is energized, however, contact 45 is momentarily closed, allowing tape-stepping magnet 27 to function. This causes the key tape to step forward to the next position. It will remain in that position until the next time relay 28 is energized.

There now remains to be described only how lever 35 is controlled.

The keyboard is provided with a universal bar, operable by every key. When a key is depressed and then released, the universal bar, near the close of its upward swing on return to normal position, actuates the lever 35, and causes it to be withdrawn from its engagement with armature 36. The latter immediately returns to its normal, retracted position, allowing contacts to be reestablished at 32 and 36. In the meantime the tape-stepping magnet

having been actuated as described above, one of two things can happen as regards the set-up of connections in key-tape transmitter 26: either a new set of connections between contact-levers and paired contacts has been established, or, by chance, if two similar characters occur in sequence on the tape, the same set of connections as before has been established. These two cases are described in turn:

(1) If a new set of connections in key-tape transmitter 26 has been established, say a set corresponding to the Baudot signal for "X", the set of connections no longer matches that set up in the cipher-wheel transmitter, 22, which, as we have seen, corresponded in the preceding case to the letter "Z". Consequently, immediately upon closing of contact at 36 under action of the universal bar, the circuit for energizing solenoid 25 is closed, allowing the cipher wheel to step forward. It will continue to do so until that set-up of pins on the rim of the cipher wheel corresponding to letter "X" presents itself to the contact-levers of the cipher-wheel transmitter, 22, whereupon relay 28 is energized, contact at 36 is broken, solenoid 25 deenergized, and the cycle has been completed.

(2) If, by chance, the next character on the key tape is the same as before ("Z" again), relay 28 is immediately energized, since the cipher-wheel transmitter is still set up for permutation "Z". Solenoid 25 does not get a chance to function and the cipher wheel is held in place. Two letters are

therefore enciphered at the same position of the cipher wheel. Of course, if the key tape now consists of a series of "Z's", the cipher wheel will remain in fixed position during the encipherment of a corresponding number of letters.

It is obvious that the permutations of perforations on the key tape as well as the permutations of operative pins on the rim of the cipher wheel must be restricted to two sets of 26 similar permutations, otherwise there would be times when the cipher wheel would continue to revolve indefinitely and no encipherment or decipherment could take place. This is true for the reason that in order to bring the cipher wheel to rest it is essential that a permutation of pins on its rim exactly coincide with that permutation which happens to be set up at the key-tape transmitter at that moment. This restriction to two sets of similar permutations does not, however, reduce the cryptographic security of the system in any degree whatsoever.

In addition, attention is especially called to the way in which a serious disadvantage of other cryptographs employing the Baudot code for cryptographic purposes is obviated in our system. In order to explain what is meant it is necessary to enter into a brief discussion of Baudot transmission from the practical, economic point of view. For this purpose we can hardly improve upon the excellent discussion to be found in U. S. patent No. 1,416,765, issued May 23, 1922, to G. S. Vernam, which is as follows:

"Arrangements have been developed for enciphering and deciphering code messages by the use of printing telegraph equipment, in which ar-

rangements the characters of a message, when in code formation, are combined in effect with the code combinations of one or more perforated key tapes and the resulting code combinations make up the characters of the enciphered message. In this device the code combinations of the enciphered or deciphered message are recorded on a perforated tape or the corresponding characters may be printed if desired and the message may then be transmitted in any desired manner to its destination.

"One of the well-known codes utilized with messages prepared by printing telegraph equipment is the Baudot code in which each character is represented by a combination of five 'marking' or 'spacing' impulses. In a five-unit code of this sort there are thirty-two different code combinations of which twenty-six are used to designate letters of the alphabet and the remaining six combinations are used as 'stunt' signals to control operations of the printing mechanism, such as 'line feed,' 'carriage return,' etc. In the above-mentioned method of enciphering messages these six 'stunt' signals will ordinarily appear at irregular intervals in the cipher message and therefore they must be recorded in some way in the written or printed form of the message. The presence of these 'stunt' signals can not be avoided by omitting them from the original message and key tapes because of the fact that they are produced by various combinations of letters in the message with letters in the key tapes. If an ordinary printer is used to record the cipher message the result would be a badly confused message due to the fact that the 'stunt' signals occur at other than the proper times. To avoid confusion of this sort printed characters must be used to represent the 'stunt' signals in the printed form of the message. It might also be possible to utilize numerals or punctuation marks for this purpose. A cipher message prepared in the above manner is not in desirable form for transmission over the ordinary commercial types of telegraph or cable lines for the following reasons. The usual practice in preparing cipher messages for transmission over commercial lines is to divide the letters into groups of five. The telegraph companies count each group of five letters as one word in charging for such messages. Mixed groups containing both letters and numerals are not accepted for transmission by cable and when transmitted over land lines each such group is counted as five words. As the numerals designating 'stunt' signals might appear frequently in the cipher message it will be seen that the charge for transmitting such a message over a commercial line would be exceedingly high."

In the patent to which reference has just been made, a special mechanism was devised to suppress the six extra characters which cause all these difficulties; and while accomplishing the object intended, the mechanism is quite complicated and has in addition the further disadvantage that the method selected to accomplish the suppression of the six extra characters results in incredasing the number of characters to be transmitted by as much as 10 to 30 per cent. In our invention, both these disadvantages have been eliminated in the simplest

manner possible, viz., by arrangements which necessitate only 26 of the 32 Baudot permutations for cryptographic purposes. So far as cryptographic technique is concerned, basically our arrangements for eliminating the six extra characters ordinarily introduced by the use of the Baudot code for cryptographic purposes differ from those described in the patent referred to above in the following respect. In the cryptographic system underlying the latter method the cipher resultants in the cryptographic process are the resultants of electrical interaction between a set of signaling elements in the Baudot code set up by a message character and a set of signaling elements in the same code set up by a key character; these resultants can not be restricted to but 26 of the 32 possible Baudot permutations because of this interaction. In our cryptographic system the cipher resultants in the cryptographic process are not at all the resultants of electrical interaction between two sets of signaling elements in the Baudot code; the signaling element representing the message character is not at all in the Baudot code and does not interact directly with the signaling elements representing the key character, nor is the cipher resultant represented by signaling elements in the Baudot code. The role the Baudot code plays in our system is, so far as signaling elements are concerned, only an indirect one, and that is why in our system the restriction of cipher characters to a set of only 26 is rendered easy, without any apparatus specifically introduced to suppress the six extra characters.

It is obvious that instead of having the cryptograph function to produce evanescent signals of the type indicated in the foregoing description, it is possible to provide at 10, Figure 1, a set of 26 solenoids, instead of a set of 26 lamps, which solenoids would act directly upon the keyboard of a typewriter with which they are associated, so as to cause the typewriter to print the letters of the cipher message, in the case of enciphering, and the letters of the plain-text message, in the case of deciphering.

Again, these solenoids, instead of being associated with the keyboard of an ordinary typewriter, might be associated with the keyboard of an automatic telegraph transmitter keyboard, and thus, in the case of enciphering, bring about the transmission of signals corresponding to enciphered letters. At the receiving end of this system, the received signals would act directly upon the keyboard of the cryptograph, and the latter would cause the received cryptographed signals to be deciphered and, if the cryptograph at the receiving end is associated with a typewriter as described in the preceding paragraph, the cryptograph would cause a written record to be made of the deciphered message.

It is also obvious that the mechanism which we have provided permits of variations in cryptographic resultants other than those introduced by changing the key tape. One of these sources of variations lies in the possibility of changing the permutations of operative and inoperative pins

on the rim of the cipher wheel. Another source lies in the changing of connections between the keyboard contacts and the contacts of plate 6, Figure 1; or between the contacts of plate 4 and the signaling elements in bank 10. Another source lies in the changing of connections between the contacts on the obverse and reverse faces of the cipher wheel. Finally, an important source of variation lies in the changing of the connections between the paired contacts of the tape transmitter, 26, and the cipher-wheel transmitter, 22. All these sources of variation existing within the mechanism itself are subsidiary, however, to the principal source inherent in constant change of key tapes, and it may be said that so long as a given key tape coextensive in number of characters with that of the intelligence to be enciphered, so that no two messages are ever enciphered by the same key tape or portion thereof, and so long as these key tapes consist of unintelligible, entirely randomized sequences of characters, the messages enciphered according to such a system are absolutely indecipherable without actual possession of the key tapes employed in their encipherment or a knowledge of the sequence of the characters on such key tapes.

We claim:

1. In a cryptograph, a 26-element keyboard comprising a set of 26 contacts for closing respective circuits to a set of 26 signaling elements, serving as a connection-changing device a rotatable cipher wheel for varying the connections between the contacts of the keyboard and the elements of the set of signaling elements, a first transmitter mechanically controlled by the cipher wheel, a second transmitter controlled by a tape bearing perforations permuted in accordance with a plural-unit code, and means, under the joint control of both first and second transmitters, for controlling the angular displacements of the cipher wheel.

2. In a cryptograph, an electrical circuit comprising a source of current, a relay, a first set of five vibrating contact levers capable of being permutatively positioned with respect to their ten associated paired contact points, and a second and similar set of contact levers and contact points, the individual contact levers and contact points of both sets being interconnected in such a manner that the circuit is completed and the relay energized at only such times as the series of connections established within the first set of contact levers and their associated contact points is identical with the series of connections established within the second set of contact levers and their associated contact points.

3. In a cryptograph, an electrical circuit comprising a source of current, a relay, a first set of five vibrating contact levers capable of being permutatively positioned with respect to their ten associated paired contact points, a second and similar set of contact levers and contact points,

the individual contact levers and contact points of both sets being interconnected in such a manner that the circuit is completed and the relay energized at only such times as the whole series of connections established within the first set of contact levers and their associated contact points is identical with the whole series of connections established within the second set of contact levers and their associated contact points, and means for permutatively varying as a set each of the two said sets of contact levers.

4. In a cryptograph, an electrical circuit comprising a source of current, a relay, a first set of five vibrating contact levers capable of being permutatively positioned with respect to their ten associated paired contact points, a second and similar set of contact levers and contact points, the individual contact levers and contact points of both sets being interconnected in such a manner that the circuit is completed and the relay energized at only such times as the whole series of connections established within the first set of contact levers and their associated contact points is identical with the whole series of connections established within the second set of contact levers and their associated contact points, and means for permutatively varying as a set each of the two said sets of contact levers, said permutative variations being in accordance with the same plural-unit code for both sets of contact levers.

5. In a cryptograph, an electrical circuit comprising a source of current, a relay, a first set of five vibrating contact levers capable of being

permutatively positioned with respect to their ten associated paired contact points, a second and similar set of contact levers and contact points, the individual contact levers and contact points of both sets being interconnected in such a manner that the circuit is completed and the relay energized at only such times as the series of connections established within the first set of contact levers and their associated contact points is identical with the series of connections established within the second set of contact levers and their associated contact points, means for permutatively varying as a set each of the two sets of contact levers, the permutative variations for one of said sets of contact levers being in accordance with one plural-unit code, those for the other of the two sets of contact levers being in accordance with a different plural-unit code.

6. In a cryptograph, a cipher wheel bearing on its rim 26 sets of pins, the sets being equidistantly spaced around the rim, each set consisting of five pins equidistantly spaced transversely to the rim, each pin being capable of being fixed in an operative or inoperative position, the five pins of each set being arranged in operative and inoperative positions according to a different permutation of a 5-unit code.

7. In a cryptograph, a rotatable cipher wheel bearing on its rim 26 sets of pins, the sets being equidistantly spaced around the rim, each set consisting of five pins equidistantly spaced transversely to the rim, each pin being

capable of being fixed in an operative and inoperative position, the five pins of each set being arranged in operative and inoperative positions according to a different permutation of a 5-unit code, the cipher wheel also bearing on its obverse and reverse faces respectively a set of 26 equidistantly spaced contact surfaces arranged in a ring on the periphery of said faces, the contact surfaces on the obverse face being connected respectively to the contact surfaces on the reverse face, the connections being fortuitously established.

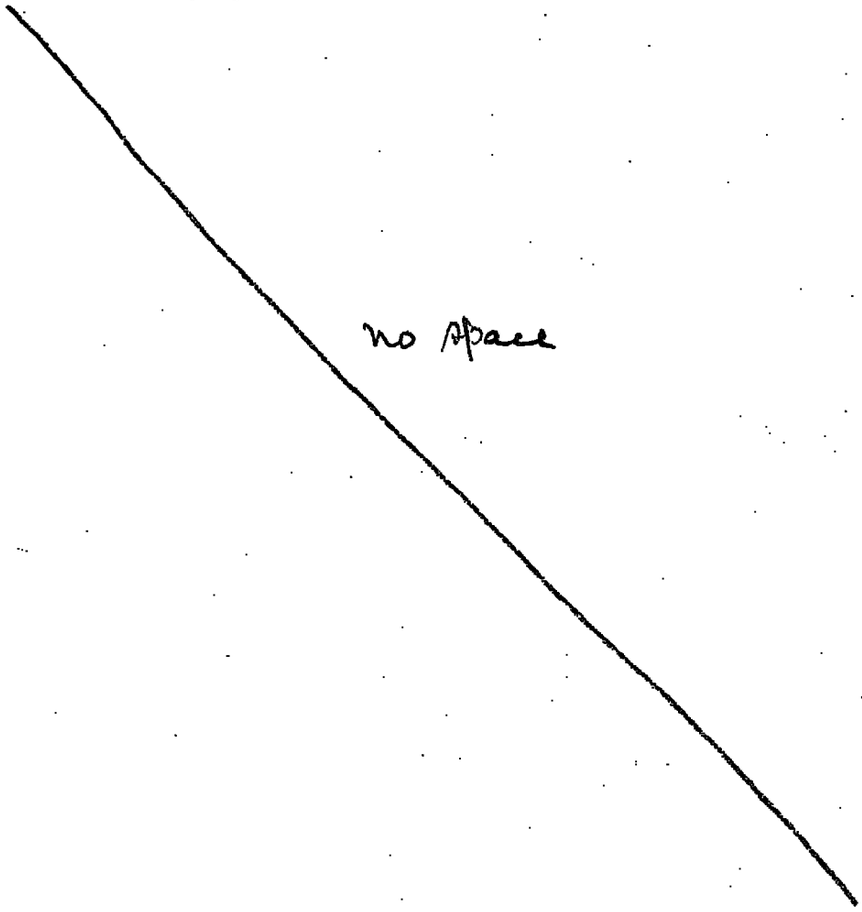
8. In a cryptograph, a rotatable cipher wheel serving as a connection-changing device bearing on its rim 26 sets of pins, the sets of pins being equidistantly spaced around the rim, each set consisting of five pins equidistantly spaced transversely to the rim, each pin being capable of being fixed in an operative and inoperative position, the five pins of each set being arranged in operative and inoperative positions according to a different permutation of a 5-unit code, the cipher wheel also bearing on its obverse and reverse faces respectively a set of 26 equidistantly spaced contact surfaces arranged in a ring on the periphery of said faces, the contact surfaces on the obverse face being connected respectively to the contact surfaces on the reverse face, the connections being fortuitously established reciprocally in pairs.

9. In a cryptograph, a relay in an electric circuit, a rotatable cipher wheel bearing on its rim 26 sets of pins, the sets of pins being equidistantly spaced around the rim, each set consisting of five pins

equidistantly spaced transversely to the rim, each pin being capable of being fixed in an operative and inoperative position, the five pins of each set being arranged in operative and inoperative positions according to a different permutation of a 5-unit code, a cipher-wheel transmitter controlled by said pins, said cipher-wheel transmitter comprising a set of ten contact points arranged in two groups of five in opposite banks between which vibrate five permutatively operable contact levers tangentially adjacent to the cipher-wheel, said contact levers under control of the pins on the rim of the cipher-wheel setting up a series of five portions of an electric current through all of the contact levers and five of their ten associated contact points.

10. In a cryptograph, a relay in an electric circuit, a rotatable cipher wheel bearing on its rim 26 sets of pins, the sets of pins being equidistantly spaced around the rim, each set consisting of five pins equidistantly spaced transversely to the rim, each pin being capable of being fixed in an operative and inoperative position, the five pins of each set being arranged in operative and inoperative positions according to a different permutation of a 5-unit code, a cipher-wheel transmitter controlled by said pins, said cipher-wheel transmitter comprising a first set of ten contact points arranged in two groups of five in opposite banks between which vibrate five permutatively operable contact levers tangentially adjacent to the cipher-wheel, said contact levers under control of the pins on the rim of the cipher-wheel setting up a first series of five portions of the circuit for operating the relay, said portions

including all of the contact levers and five of their ten associated points, a perforated-tape transmitter controlling a second set of ten contact points arranged in two groups of five in opposite banks between which vibrate five permutatively operable contact levers thus setting up a second series of five portions of the same circuit for operating the relay, said portions including all of said contact levers and five of their ten associated contact points, the various elements of said first and second series of portions of the circuit for operating the relay being interconnected in such a manner as to form a continuous path for the passage of the current only under certain specified conditions as regards the permutative positions of the first and second sets of permutatively operable contact levers.



11. In a cryptograph, the combination of a cipher-wheel transmitter, a rotatable cipher wheel bearing on its rim 26 sets of pins capable of being arranged, as regards their being in operative and inoperative positions on the rim, permutatively in groups of five in accordance with 26 of the 32 permutations of a 5-unit code to control the cipher-wheel transmitter, and a tape transmitter.

12. In a cryptograph, the combination of a cipher-wheel transmitter, a rotatable cipher wheel bearing on its rim 26 sets of pins capable of being arranged, as regards their being in operative and inoperative positions on the rim, permutatively in groups of five in accordance with 26 of the 32 permutations of a 5-unit code to control the cipher-wheel transmitter, and a tape transmitter, said tape transmitter, under the control of a perforated, key tape which is passed through the transmitter, and said cipher-wheel transmitter jointly controlling the angular displacements of the cipher wheel in enciphering or deciphering messages.

13. In a cryptograph employing in combination a cipher-wheel transmitter, a rotatable cipher wheel which bears on its rim 26 sets of pins capable of being arranged, as regards their being in operative and inoperative positions on the rim, permutatively in groups of five according to 26 of the 32 permutations of a 5-unit code to control the cipher-wheel transmitter, and a perforated, key-tape transmitter, means by which said transmitters jointly control the angular displacements of said cipher wheel in enciphering or deciphering messages.

14. In a cryptograph employing in combination a cipher-wheel transmitter, rotatable cipher wheel which bears on its rim 26 sets of pins capable of being arranged, as regards their being in operative and inoperative positions on the rim, permutatively in groups of five according to 26 of the 32 permutations of a 5-unit code to control the cipher-wheel transmitter, and a perforated, key-tape transmitter, means by which said transmitters jointly control the angular displacements of said cipher wheel in enciphering or deciphering messages, said means consisting of a motor-driven coiled spring, a ratchet associated with the cipher wheel, a solenoid, the armature of which acts on the ratchet and permits the cipher wheel to be displaced angularly in stepwise fashion, the solenoid being actuated by means under the joint control of the cipher-wheel transmitter and the perforated, key-tape transmitter.

15. In a cryptograph employing in combination a cipher-wheel transmitter, rotatable cipher wheel which bears on its rim 26 sets of pins capable of being arranged, as regards their being in operative and inoperative positions on the rim, permutatively in groups of five according to 26 of the 32 permutations of a 5-unit code to control the cipher-wheel transmitter, and a perforated, key-tape transmitter, means by which said transmitters jointly control the angular displacements of said cipher wheel in enciphering or deciphering messages, said means consisting of a motor-driven coiled spring,

a ratchet attached to the cipher wheel, a solenoid, the armature of which acts on the ratchet and permits the cipher wheel to be displaced angularly in stepwise fashion, the solenoid being actuated by means under the joint control of the cipher-wheel transmitter and the perforated, key-tape transmitter, said joint control being according to the rule that the cipher wheel under the drive of the motor-driven coiled spring is caused to be displaced angularly in stepwise manner by the solenoid, the latter acting in conjunction with the ratchet until the permutation of pins on the rim of the cipher wheel sets up in the cipher-wheel transmitter a first set of five portions of an electrical path through a first set of five of a group of ten paired contact points and associated five contact levers comprising said cipher-wheel transmitter, said first set of five portions of an electrical path exactly matching a second and similar set of five portions of another part of the same electrical path through a second set of five of a group of ten paired contact points and associated five contact levers controlled by the tape transmitter, whereupon the cipher wheel is halted in its rotation.

16. In a cryptograph employing in combination a bank of 26 signaling elements, a 26-element keyboard comprising a set of 26 contacts for closing respective circuits to the set of signaling elements, a plural-unit-code key-tape transmitter jointly controlling with the keyboard the set of signaling elements, means for changing the electrical paths between the elements of

the keyboard and the elements of the bank of signaling elements, said means consisting of a cipher wheel with a first set of 26 contacts equidistantly distributed on the obverse face of the cipher wheel, a second and homologous set of 26 contacts equidistantly distributed on the reverse face of the cipher wheel, insulated conductors passing through the cipher wheel and connecting the contacts of the obverse face respectively with the contacts of the reverse face, on the rim of the cipher wheel 26 sets of pins capable of being arranged in operative and inoperative positions according to the permutations of a 5-unit code, a cipher-wheel transmitter comprising a first set of five vibrating contact levers actuated by the permutatively positioned pins on the rim of the cipher wheel to set up through the contact levers and five of their associated ten paired contact points a first set of five portions of an electrical path for the control of the angular displacement of the cipher wheel, a second set of five vibrating contact levers actuated by the plural-unit-code key-tape transmitter to set up through the five key-tape transmitter contact levers and five of their associated ten paired contact points a second set of five portions of another part of the same electrical path for the control of the angular displacement of the cipher wheel, means for imparting to the cipher wheel a rotatory movement, latter means being under control of said electrical path, said control being according to the rule that the angular displacement of the cipher wheel continues until the first set of five portions of said electrical path exactly matches the second set of portions.

17. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externally controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated.

18. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externalling controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random sequence of characters in a plural-unit-code.

19. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externally controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible,

random sequence of characters in a plural-unit-code; and constantly changing said tape.

20. In a cryptograph, the method of enciphering which consists in continously varying the cipher resultant of a given plain-text character by externalling controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random sequence of characters in a plural-unit-code; constantly changing said tape; and making said tape coextensive in length with the length of the message to be enciphered.

21. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externally controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random sequence of characters in a plural-unit-code; constantly changing said tape; and making said tape coextensive in length

with the total lengths of the set of messages to be enciphered.

22. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externally controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random sequence of characters in a plural-unit code; constantly changing said tape; making said tape coextensive in length with the total lengths of the set of messages to be enciphered; and constantly changing said tape with each different set of messages.

23. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externally controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random sequence of characters in a plural-unit-code; and causing said transmitter to operate jointly with means under control

of said connection-changing device.

24. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externally controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random sequence of characters in a plural-unit-code; and causing said transmitter to operate jointly with means under control of the connection-changing device, latter means consisting of a transmitter controlled by pins projecting from the rim of the connection-changing device.

25. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by externally controlling the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain text character is established and the element upon which the cipher character is indicated, said external control consisting in using an electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random sequence of characters in a plural-unit-code; causing said transmitter to operate jointly with means under control of said connection-changing device, latter means consisting of a transmitter con-

trolled by pins projecting from the rim of the connection-changing device; and causing said pins to be arranged in sets in operative and inoperative positions corresponding to permutations of a plural-unit-code.

26. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by exercising a two-phase control over the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is established; causing one phase of said two-phase control to be exercised by an element which is external to the cryptograph itself; and causing the other phase to be exercised by an element which is a member of the cryptograph.

27. In a cryptograph, the method of enciphering which consists in continuously varying the cipher resultant of a given plain-text character by exercising a two-phase control over the angular displacements of a rotatable, cylindrical connection-changing device interposed between the element upon which the plain-text character is established and the element upon which the cipher character is established; causing one phase of said two-phase control to be exercised by an element which is external to the cryptograph itself, said phase consisting in using a first electrical transmitter through which is passed a perforated tape bearing perforations corresponding to an unintelligible, random

sequence of characters in a plural-unit code; causing the other phase of said two-phase control to be exercised by an element which is internal to the cryptograph itself, the latter phase consisting in using a second electrical transmitter controlled by pins which project from the rim of the connection-changing device, said pins being arranged in permutations corresponding to 26 letters of a plural-unit code; and causing the first and second transmitters to interact in jointly controlling a solenoid, said solenoid being so positioned and actuated as to control the successive angular displacements of the connection-changing device.

28. In a cryptograph employing as one of its keying elements a tape transmitter through which is passed a key tape bearing perforations permuted in accordance with a five-unit code, the method of eliminating from the final cryptograms those six permutations of said code which have no standard equivalents in the Morse code, said method consisting in causing the key-tape transmitter to interact with a second transmitter which is entirely independent of control by the message character.

29. In a cryptograph employing as one of its keying elements a tape transmitter through which is passed a key tape bearing perforations permuted in accordance with a five-unit code, the method of eliminating from the final cryptograms those six permutations of said code which have no standard equivalents in the Morse code, said method consisting in causing said key-tape transmitter to serve as a means of opening and closing a set of five in-

dependent circuit breaking elements of a single electrical circuit having a set of ten such independent circuit-breaking elements.

30. In a cryptograph employing a first transmitter controlled by a rotatable, cylindrical connection-changing device and a second transmitter controlled by a perforated key tape bearing perforations permuted in accordance with a five-unit code, said key tape serving as the keying element for ciphering, the method of eliminating from the final cryptograms those six permutations of said five-unit code which have no standard equivalents in the Morse code, said method consisting in causing both transmitters to serve jointly as a means of opening and closing a single electrical circuit having ten independent circuit-breaking elements arranged in two sets of five, the first set being controlled by one of said transmitters, the second set being controlled by the other transmitter.

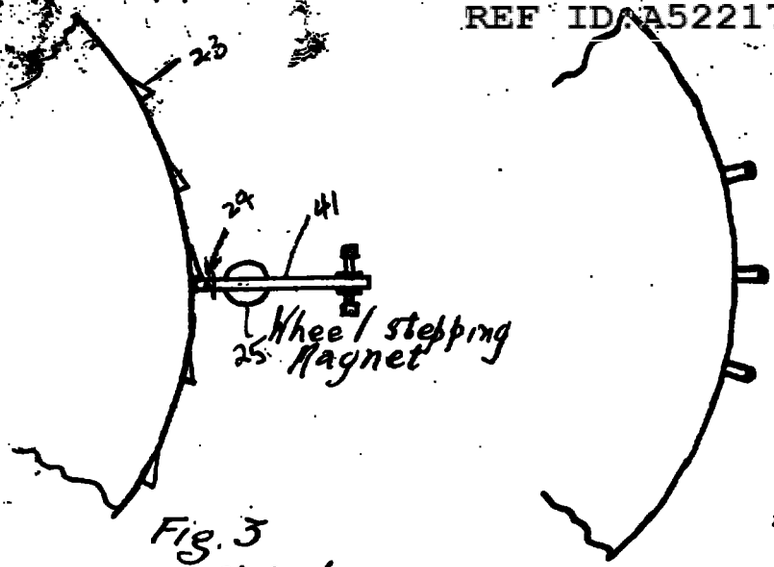


Fig. 3
Plan of Wheel stepping Pawl

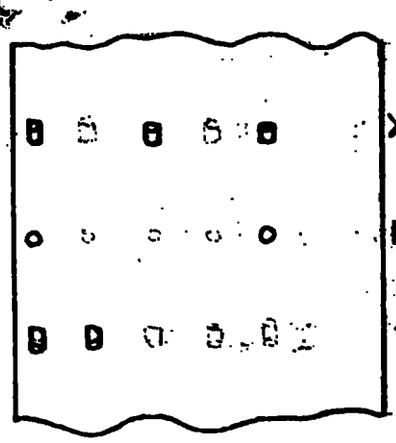


Fig. 2.

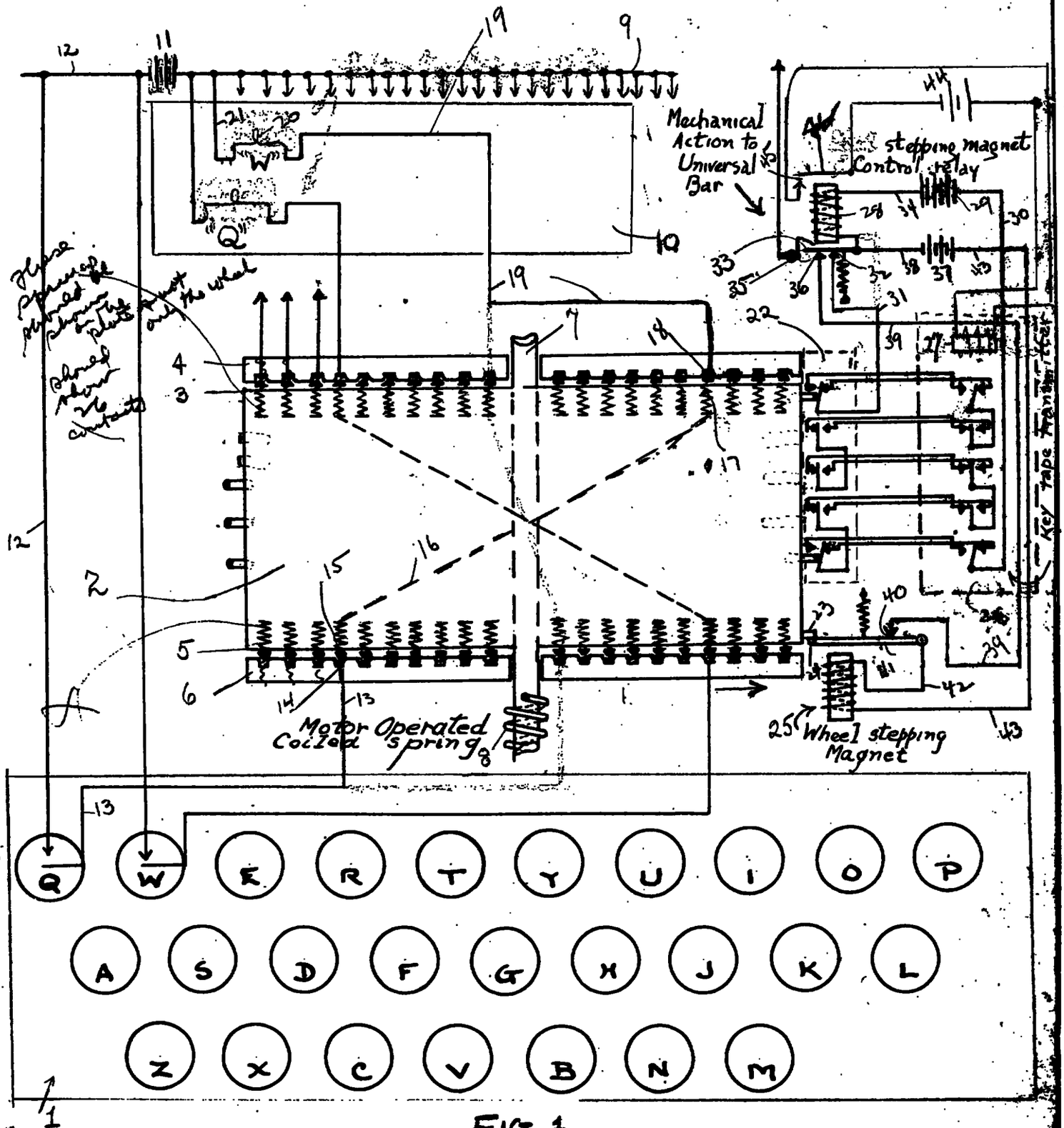


Fig. 1